AO 106 (Rev. 06/09) Application for a Search Warrant

FILED

SEP 30 2021

Mark C. McCartt, Clerk
U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
INFORMATION ASSOCIATED WITH LOVEJOYBABY@ICLOUD.COM, MORGANCALDWELL1517@GMAIL.COM, and PAULDEMARCO510@PROTONMAIL.COM, STORED AT PREMISES CONTROLLED BY APPLE INC.

Case No. 21-MJ-704-JFJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2422	Coercion and Enticement
18 U.S.C. §§ 2251(a)	Sexual Exploitation of Children
18 U.S.C. § 2252(a)(2)(A) and (B)	Receipt of Child Pornography
18 U.S.C. §§ 2252(a)(4)(B) and (b)(2)	Possession of child Pornography

The application is based on these facts:

See Affidavit of Brian S. Dean, attached hereto.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Brian S. Dean, FBI
Printed name and title

Sworn before me via phone

Date: 9/30/21

Judge's signature

City and state: Tulsa, OK

Jodi F. Jayne, U.S. Magistrate
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Brian S. Dean, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID's stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Apple Park Way, Cupertino, California, 95014. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) assigned to the Oklahoma Safe Trails Task Force based out of Tulsa, OK. As a Special Agent, my duties include investigating violations of federal criminal law and threats to national security. In addition to formalized training, I have received extensive training through my involvement in numerous investigations working alongside experienced law enforcement officers at both the federal and local level. My investigations include, but are not limited to, drug and gang violations, violent crimes, counterterrorism, computer intrusion, Indian Country crimes, and crimes against children.

3. The facts and circumstances of this investigation set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the circumstances described herein, and a review of open-source information. This affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, and therefore does include every fact I have learned during the course of this investigation.

4. Based on my training, research, experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of:

- 18 U.S.C. § 2422 – Coercion and Enticement
- 18 U.S.C. §§ 2251(a) – Sexual Exploitation of Children
- 18 U.S.C. § 2252(a)(2)(A) and (B) – Receipt of Child Pornography,
- 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) – Possession of child Pornography,

have been committed, and evidence of these crimes, as set forth in Attachment B, are located in the accounts as further described in Attachment A.

DEFINITIONS

5. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where

a. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

b. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

c. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct

6. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

7. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

8. The term "computer," as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

9. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

CHARACTERISTICS COMMON TO INDIVIDUALS WITH INTENT TO COLLECT, RECEIVE OR DISTRIBUTE CHILD PORNOGRAPHY

10. Based on my previous experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals with intent to view and/or possess, collect, receive, or distribute images of child pornography:

a. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children

oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Likewise, individuals with intent to view and/or possess, collect, receive, or distribute pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

d. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND REGARDING CHILD PORNOGRAPHY AND TECHNOLOGY

11. Computers and computer technology have revolutionized the way in which child pornography and other depictions of children being sexually exploited is produced, distributed, stored, and utilized. It has also revolutionized the way in which collectors interact with each other. Child pornography was formerly produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill to develop and

reproduce the images. As a result, there were definable costs involved with the production of pornographic images, and even greater costs associated with their distribution.

12. The development of computers, mobile devices, and the Internet however drastically changed the means by which people produce, gain access to, and distribute child pornography. Child pornography can now be reproduced inexpensively, marketed anonymously (through electronic communications), and distributed to anyone with access to a computer and modem. In addition, the proliferation of commercial services that provide easy access to the Internet and electronic sharing and storage systems (IE. Email, Instant Messaging, Social Media, etc.) has made mobile devices and computers the preferred methods of distribution and receipt of child pornographic materials.

BACKROUND REGARDING APPLE ID AND ICLOUD

13. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

14. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). The services include email, instant messaging, and file storage:

- Apple provides email service to its users through email addresses at the domain names including, but not limited to mac.com, me.com, and icloud.com.
- iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.
- iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.
- iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the

Safari web browsers on all the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

- Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.
- Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.
- Find My Friends allows owners of Apple devices to share locations.
- Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.
- App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through

iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

15. Apple services are accessed through an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

16. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) typically after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

17. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of

service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

18. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

19. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the

unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding specific Apple devices or services, and the repair history for said devices.

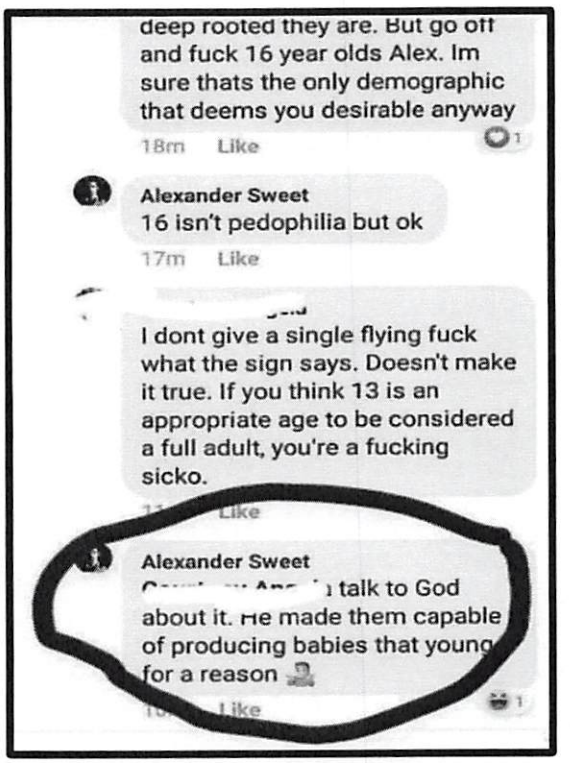
20. Apple provides users with approximately five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud

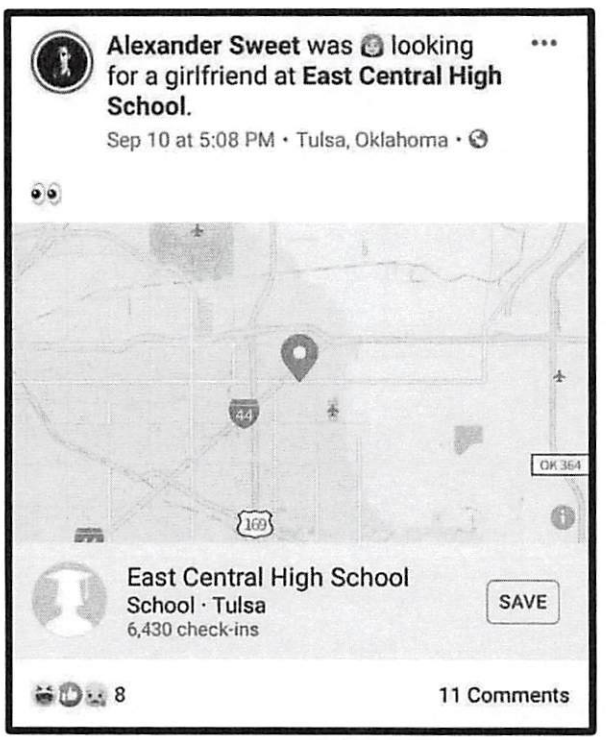
Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

INVESTIGATIVE BACKGROUND

21. In December 2020, FBI Tulsa received information a 27-year-old man by the name of ALEXANDER SWEET was in an intimate relationship with a 16-year-old girl, hereinafter referred to as Victim 1 and was in possession of graphic photographs and videos constituting child pornography. Law enforcement personnel were separately provided with screen shots from a witness (herein identified as Witness 1) of several social media posts he/she believed to be made by SWEET. The posts were made across an array of social media platforms and specifically discussed SWEET's sexual interest in minor girls. Several examples are provided below:


People are still sending me death threats because I was with a 16 year old this year? Lol wow.
10 likes
alexnsweet So I'm into younger girls. To each their own. The world goes on. Love and let live. #single #Oklahoma


deep rooted they are. But go off and fuck 16 year olds Alex. Im sure thats the only demographic that deems you desirable anyway
18m Like
Alexander Sweet
16 isn't pedophilia but ok
17m Like
I dont give a single flying fuck what the sign says. Doesn't make it true. If you think 13 is an appropriate age to be considered a full adult, you're a fucking sicko.
Like
Alexander Sweet
talk to God about it. He made them capable of producing babies that young for a reason
Like


Alexander Sweet was looking for a girlfriend at East Central High School.
Sep 10 at 5:08 PM • Tulsa, Oklahoma •
44
OK 364
169
East Central High School
School · Tulsa
6,430 check-ins
SAVE
8
11 Comments

Agents subsequently identified Victim 1 and set up a time for her to be interviewed by an FBI Child / Adolescent Forensic Interviewer (CAFI). The interview took place at the Child Advocacy Center in Tulsa, OK and was monitored by your affiant.

22. During the interview, Victim 1 said she was initially contacted by SWEET on Instagram in September 2019 when she was 15 years old. Victim 1 said SWEET sent her an edited nude photograph she originally sent to her ex-boyfriend. SWEET told her he found it online and wanted her to be aware it had been posted. Victim 1 said she communicated with SWEET off and on via social media for several months, but did not meet him in person until mid-2020. Victim 1 said she lost her grandfather to cancer in January 2020 and her father to suicide in February 2020 and was feeling very alone before she and SWEET started dating in September of 2020.

23. Over the course of the relationship, Victim 1 said she sent a significant number of sexually graphic photographs and videos to SWEET across multiple social media platforms using several different applications. Victim 1 said among other things, the images she sent included pictures and videos of her genitalia, and on several occasions, she live streamed herself taking a shower to SWEET on the Google Meet / Google Hangout application. A number of these videos were taken and sent from her bedroom and bathroom which is located in the Northern District of Oklahoma. Victim 1 said she mainly used her school laptop, issued to her by Epic Charter Schools, to send the images as opposed to her cellphone because her mother did not allow her to have her phone when she went upstairs to bed. Pursuant to a

federal search warrant, filing number 20-MJ-510-PJC, issued on or about 22 December 2020 in the Northern District of Oklahoma, law enforcement officers seized a black Lenovo Chromebook matching the description provided by Victim 1 from a bedroom where Victim 1 was alleged to have stayed, and submitted it for forensic examination.

24. On January 4, 2021, law enforcement officers contacted Epic Charter School's Technical Support in reference to the laptop. The Technical Support Manager said he was unable to access the majority of user account information from his administrative role because most of it was stored via Google's servers in accordance with the school's Chromebook usage agreement. The Technical Support Manager was however able to confirm the laptop had been issued to Victim 1 and had been used to connect via Google Meets / Google Hangouts on multiple occasions with several accounts bearing the display name "Alexander Sweet."

25. Additional open-source research identified the following Google accounts associated with display name "Alexander Sweet": alexnsweet@gmail.com and alexandernsweet@gmail.com. On February 22, 2021, law enforcement personnel submitted 2703(d) Order 21-MJ-115-JFJ to Google requesting subscriber information for the identified accounts, as well as any additional linked accounts. On April 6, 2021, Agents downloaded and began review of a zip file provided by Google via their law enforcement portal containing information associated with the accounts. During the review, Agents identified several additional accounts which shared the recovery e-mail address of alex_sweet_2000@hotmail.com and or were

connected by "cookie."[1] As such, on May 27, 2021, law enforcement personnel submitted federal search warrant 21-MJ-430-CDL to Google via their law enforcement portal for the identified accounts, to include alexnsweet@gmail.com.

26. On June 30, 2021, Google responded with several encrypted files containing information associated with the specified target accounts. During a cursory review, Agents discovered numerous items of evidentiary value, to include, but not limited to:

- A sexually explicit video depicting Victim 1. Metadata confirms the video was created at Victim 1's residence on or about September 27, 2020, and is consistent with what she disclosed in the forensic interview. The video was discovered within a Google Photos folder connected to alexnsweet@gmail.com.

- A screen shot of a live "Google Hangouts" conversation between whom Agents believe to be SWEET and Victim 1 depicting both parties engaged in self stimulation. The photo was discovered within a Google Photos folder connected to alexnsweet@gmail.com and had a pathway which contained Victim 1's name.

- Subscriber information for alexnsweet@gmail.com lists a phone number known to be utilized by SWEET as a Sign-In Phone Number, a Reachable Phone Number, and a 2-Step Verification Phone Number.

[1] A "recovery" email or phone number is often required by electronic communication providers such as Google as part of their protection protocols. This "recovery" option provide users with a secure means of regaining access to their account should they forget their password. In choosing an alternate or recovery e-mail and/or phone number, individuals typically use an account which they control completely. This account is then verified through a message containing a code or link which users must enter or visit to confirm they have access to the alternate account. Accounts linked by cookies indicates they were logged into from the same device while the same browser cookie was present, suggesting the accounts were being accessed by the same individual. Based on my training and experience, individuals involved in criminal behavior such as the possession of child pornography often utilize multiple e-mail accounts to compartmentalize and obfuscate their activity.

27. Google LLC is an electronic communications provider headquartered in Mountain View, California, and is a means and facility of interstate and international commerce. Users of Google services can receive and or transmit data, to include photographs and videos, to other users and Google's servers utilizing the Internet. Victim 1's Lenovo laptop seized by Agents and used to communicate with SWEET was not manufactured in the state of Oklahoma and thus traveled in interstate commerce.[2] Additionally, open-source research indicates no cell phones currently on the market are produced and or manufactured in the state of Oklahoma, therefore any cellular device used to communicate with SWEET also traveled in interstate commerce.

ARREST OF SWEET

28. On 22 July 2021, the FBI received information SWEET planned to leave the state later that day and was taking Victim 1 with him. Agents were provided with a photograph reportedly taken earlier in the day depicting SWEET's current vehicle (red sedan) and his current clothing (gray t-shirt).

29. While conducting surveillance, Agents located a red Ford Focus bearing South Dakota tag 2AD061 near the QuikTrip at the intersection of 21st and Sheridan. Notably, the writing "Just Married" was visible on the car's rear windshield. These observations correlated with information previously discovered

[2] Based on open source research, Lenovo does not have any locations or facilities in the state of Oklahoma (source: https://www.lenovo.com/us/en/about/locations)

during the investigation.[3] Vehicle registration information confirmed ALEXANDER NICHOLAUS SWEET was the owner.

30. Agents observed SWEET's vehicle pulling into a parking spot in front of E-Z Pawn located at or around 2198 S. Sheridan Road, Tulsa, OK. Approximately 15 minutes later, Agents observed an individual matching SWEET's physical description exit the store and enter the driver's seat of the vehicle, and a small female enter the front passenger's seat.

31. In coordination with the Tulsa Police Department, Officers and FBI Agents conducted a felony car stop of SWEET's vehicle in the parking lot at or around 2144 S. Sheridan Road, Tulsa, OK. A probable cause arrest of SWEET was conducted, and he was subsequently transported to the David L. Moss Correctional Center pending his Initial Appearance in the Northern District of Oklahoma. Victim 1 was identified as the passenger and later released to the custody of his/her guardian.

EVIDENCE IN SWEET'S VEHICLE

32. Based on my training and experience, I know the following information about the wiping capabilities of electronic devices:

a. Electronic communication service providers such as Google and Apple offer users the capability to remotely lock or wipe devices which have been lost or stolen.

[3] In January 2021, a law enforcement database associated SWEET with an address in South Dakota connected to Escapees RV Club. The FBI later confirmed SWEET obtained a South Dakota Driver's License. Additionally, Agents were aware SWEET had filed an application for marriage in Payne County, Oklahoma the week prior.

b. Devices such as phones, computers, and tablets are capable of being remotely wiped when cellular, WiFi, and/or Bluetooth connections are enabled.

c. An electronic device typically contains little, if any, useful evidence when it has been wiped.

33. To prevent the possible destruction of evidence via remote wiping, Agents conducted a cursory search of the vehicle to locate devices such as phones, computers, or tablets. During the search for these types items, other electronic storage devices such as flash drives were also located and seized. Agents verified the seized devices were turned off, powered down, and/or in Airplane Mode. The following items were seized from SWEET's vehicle and/or keychain by law enforcement officers:

- APPLE IPHONE, ROSE GOLD, NO IDENTIFIERS
- LENOVO YOGA LAPTOP, MODEL: 80QD, S/N: PF0IC0NW
- PINK APPLE IPHONE S IN PINK LEOPARD PRINT CASE
- APPLE IPOD, MODEL A2178, S/N: F6KDQ4W8M93D
- APPLE MACBOOK PRO, MODEL: A2289, FCCID: BCGA2289 WITH CHARGER
- 128GB PNY THUMBDRIVE

34. Additionally, one (1) MICRO SD CARD IN GOODRAM ADAPTER was located on SWEET's person while in the booking area of the David L. Moss Criminal Justice Center and consequently seized.

35. The aforementioned Devices were subsequently transported to the FBI's Tulsa Resident Agency and Allied Towing of Tulsa, a company contracted by TPD, towed SWEET's vehicle to its storage facility located within the Northern District of Oklahoma. Law enforcement personnel followed up with federal search warrants 21-MJ-530-CDL and 21-MJ-531-CDL for the electronic devices and SWEET's vehicle. During initial review, several of the electronic items including the APPLE IPHONE, ROSE GOLD, NO IDENTIFIERS and the PINK APPLE IPHONE S IN PINK LEOPARD PRINT CASE were found to be encrypted and or password protected, and so they were submitted for additional forensic evaluation. During the subsequent extraction process, FBI Forensic Examiners were able to determine a number of attributable accounts associated with each phone. The APPLE IPHONE, ROSE GOLD, NO IDENTIFIERS was connected to **LOVEJOYBABY@ICLOUD.COM** (hereinafter **TARGET ACCOUNT 1** or **TA1**) as well as **MORGANCALDWELL1517@GMAIL.COM** (hereinafter **TARGET ACCOUNT 2** or **TA2**); and the PINK APPLE IPHONE S IN PINK LEOPARD PRINT CASE was connected to **PAULDEMARCO510@PROTONMAIL.COM** (hereinafter **TARGET ACCOUNT 3** or **TA3**). It should be noted the extraction process is still currently ongoing.

36. In my training and experience, stored communications and files connected to the targeted accounts may provide direct evidence of the offenses under investigation. In addition to the actual content of said communications, the user's

account activity, date-time logs, geo-location data, and other information retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is critical because individuals engaged in criminal cyber activity will often register accounts with false information to obfuscate their true identity. It also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation, and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. Alternatively, this same information may help to exclude the innocent from further suspicion.

37. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation, their motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), and or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

38. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

39. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

40. Based on the above aforementioned facts and circumstances, there is probable cause to suggest the targeted accounts:

- LOVEJOYBABY@ICLOUD.COM
- MORGANCALDWELL1517@GMAIL.COM
- PAULDEMARCO510@PROTONMAIL.COM

contain evidence, fruits, and or instrumentalities of violations of statutes as previously noted. It is therefore respectfully requested this Court issues a search warrant for the location listed in Attachment A and the items listed in Attachment B.

41. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully Submitted,

Brian S. Dean
Special Agent
Federal Bureau of Investigation

Subscribed and Sworn via Phone on this 30th day of September, 2021.

JODI F. JAYNE
United States Magistrate Judge

ATTACHMENT A – PROPERTY TO BE SEARCHED

This warrant applies to information associated with

LOVEJOYBABY@ICLOUD.COM,

MORGANCALDWELL1517@GMAIL.COM, and

PAULDEMARCO510@PROTONMAIL.COM (Target Accounts 1-3) stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., One Apple Park Way, Cupertino, California, 95014.

ATTACHMENT B – ITEMS TO BE SEIZED

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"),

Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from August of 2019 through present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from August of 2019 through present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud account from August of 2019 through present, including all iOS device backups, all Apple

and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers) account from August of 2019 through present, including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations account from August of 2019 through present where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple account from August of 2019 through present and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes as fruits, evidence and/or instrumentalities of violations of 18 U.S.C. § 2422 (Coercion and Enticement), 18 U.S.C. §§ 2251(a) (Sexual Exploitation of Children), 18 U.S.C. § 2252(a)(2)(A) and (B) (Receipt of Child Pornography), and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of Child Pornography) including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence indicating other accounts used by the owner of the Apple ID

b. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

c. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

d. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

e. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

f. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.